CLMPTO

03-29-04

MBL

CLAIMS 1-22 CANCELED

CLAIMS 23-42 ADDED

Claims 1-22 (canceled)

Claim 23 (new): A method of alerting a device in a networked computer system to an anomaly, comprising:

determining that the device is anticipated to be affected by an anomaly by using network-based intrusion detection techniques comprising analyzing data entering into a plurality of hosts, servers, and computer sites in the networked computer system and by using pattern correlations across the plurality of hosts, servers, and computer sites; and

sending an alert to the device that the anomaly is anticipated at the device.

Claim 24 (new): The method of claim 23, further comprising adjusting a firewall of the device that is anticipated to be affected by the anomaly.

Claim 25 (new): The method of claim 23, wherein the anomaly comprises one of an intrusion and an intrusion attempt.

Claim 26 (new): The method of claim 23, wherein determining that the device is anticipated to be affected by the anomaly comprises analyzing a plurality of data packets with respect to predetermined patterns.

Claim 27 (new): The method of claim 26, wherein analyzing the data packets comprises analyzing data packets that have been received by at least two devices in the networked computer system.

Claim 28 (new): The method of claim 23, wherein determining that the device is anticipated to be affected by the anomaly comprises recognition of an intrusion and further comprising generating an automated response to the intrusion.

Claim 29 (new): A method of anticipating a device in a networked computer system is to be affected by an anomaly, comprising:

detecting an anomaly at a first device in the computer system using network-based intrusion detection techniques comprising analyzing data entering into a plurality of hosts, servers, and computer sites in the networked computer system; and

determining a device that is anticipated to be affected by the anomaly by using pattern correlations across the plurality of hosts, servers, and computer sites.

Claim 30 (new): The method of claim 29, wherein networked computer system comprises a plurality of devices, and the plurality of devices are polled in a predetermined sequential order, the first device being polled prior to detecting the anomaly, and the device anticipated to be affected by the anomaly is a device that has not been polled.

Claim 31 (new): The method of claim 29, further comprising transmitting an anomaly warning from the first device to a central analysis engine, responsive to detecting the anomaly at the first device, the anomaly warning comprising a unique device identifier.

Claim 32 (new): The method of claim 29, wherein the anomaly comprises one of an intrusion and an intrusion attempt.

Show First Page

Claim 33 (new): The method of claim 29, wherein detecting the anomaly comprises analyzing a plurality of data packets with respect to predetermined patterns.

Claim 34 (new): The method of claim 33, wherein analyzing the data packets comprises analyzing data packets that have been received by at least two devices in the networked computer system.

Claim 35 (new): The method of claim 29, further comprising controlling the device that is anticipated to be affected by the anomaly.

Claim 36 (new): A computer-readable medium having computer-executable components comprising a data collection and processing center monitoring data communicated to a network, and detecting an anomaly in the network using network-based intrusion detection techniques comprising analyzing data entering into a plurality of hosts, servers, and computer sites in the networked computer system.

Claim 37 (new): The computer-readable medium of claim 36, wherein the data collection and processing center determines which of a plurality of devices that are connected to the network are anticipated to be affected by the anomaly by using pattern correlations across the plurality of hosts, servers, and computer sites, and alerting the devices.

Claim 38 (new): The computer-readable medium of claim 36, wherein the data collection and processing center further determines which of a plurality of devices that are connected to the network have been affected by the anomaly and alerts the devices.

Claim 39 (new): The computer-readable medium of claim 36, wherein the data collection and processing center further adjusts a firewall of each of a plurality of devices that is connected to the network that is anticipated to be affected by the anomaly responsive to the detection of the anomaly.

Claim 40 (new): The computer-readable medium of claim 36, wherein the anomaly comprises one of an intrusion, an intrusion attempt, and reconnaissance activity.

Claim 41 (new): The computer-readable medium of claim 36, wherein the data collection and processing center detects the anomaly by analyzing a plurality of data packets with respect to predetermined patterns.

Claim 42 (new): The data collection and processing of claim 41, wherein the data collection and processing center analyzes data packets that have been received by at least two devices that are connected to the network.